(51) Int. Cl.²: G 07 C 9/00
B 44 F 1/12
B 42 D 15/02
G 06 K 19/08
G 07 F 7/08

(19) BUNDESREPUBLIK DEUTSCHLAND
DEUTSCHES PATENTAMT

DE 28 02 430 A 1

(11) Offenlegungsschrift 28 02 430

(21) Aktenzeichen: P 28 02 430.8
(22) Anmeldetag: 20. 1. 78
(43) Offenlegungstag: 27. 7. 78

(31) Unionspriorität:
(32) (33) (31) 24. 1. 77 Schweiz 824-77

(54) Bezeichnung: Identifikationsverfahren und -einrichtung

(71) Anmelder: Gretag AG, Regensdorf, Zürich (Schweiz)

(74) Vertreter: Berg, W.J., Dipl.-Chem. Dr.rer. nat.; Stapf, O., Dipl.-Ing.;
Schwabe, H.-G., Dipl.-Ing.;
Sandmair, K., Dipl.-Chem. Dr.jur. Dr.rer.nat.; Pat.-Anwälte,
8000 München

(72) Erfinder: Ehrat, Kurt, Dipl.-Ing., Steinmaur (Schweiz)

DE 28 02 430 A 1

2802430

Patentansprüche

1. Identifikationsverfahren unter Verwendung einer zwei maschinell lesbare Informationen tragenden Kennkarte, auf der die eine Information permanent und die andere Information veränderbar gespeichert ist, dadurch gekennzeichnet, dass die veränderbare, im folgenden Identifikationsinformation genannte Information bei der Erstellung der Karte durch Chiffrierung aus zumindest ausgewählten Teilen der auf der Karte vorhandenen permanenten Information und einer geheimen Schlüsselinformation gebildet und auf der Karte gespeichert wird, und dass bei der Prüfung der Karte aus denselben ausgewählten Teilen der permanenten Information und der geheimen Schlüsselinformation eine Prüfinformation gebildet und auf Uebereinstimmung mit der auf der Karte gespeicherten Identifikationsinformation geprüft wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass zur Bildung der Identifikationsinformation eine weitere, von Fall zu Fall verschiedene (variable) Zusatzinformation verwendet und unverschlüsselt vorzugsweise nach demselben physikalischen Prinzip wie die Identifikationsinformation auf der Kennkarte gespeichert wird, und dass bei der Prüfung der Karte die darauf gespeicherte Zusatzinformation zusammen mit wenigstens den ausgewählten Teilen der permanenten Information und der geheimen Schlüsselinformation zur Bildung der Prüfinformation herangezogen wird.

3. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass bei der Erstellung und der Prüfung der Kennkarte aus der geheimen Schlüsselinformation und wenigstens der Zusatzinformation durch Chiffrierung eine Auswahlinformation gebildet wird, aufgrund welcher die für die Chiffrierung heranzuziehenden Teile der permanenten Information ausgewählt werden.

4. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass zur Bildung der Identifikationsinformation und der Prüfinformation zusätzlich eine Geheiminformation, insbesondere eine Gedächtnisinformation verwendet wird.

5. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass bei Verwendung der Kennkarte als Datenträger die Dateninformation mittels der Identifikationsinformation chiffriert und in chiffrierter Form und vorzugsweise nach demselben physikalischen Prinzip wie die Identifikationsinformation auf der Kennkarte gespeichert wird, und dass bei der Prüfung der Kennkarte die Klardateninformation durch Dechiffrierung mit der Identifikationsinformation wiedergewonnen wird.

6. Verfahren nach einem der voranstehenden Ansprüche, dadurch gekennzeichnet, dass bei jeder Prüfung der Kennkarte ein Teil der permanenten Information irreversibel gelöscht und die sich aus dem Löschzustand der permanenten Information ergebende Löschinformation ebenfalls zur Bildung der Identifikationsinformation und der Prüfinformation herangezogen wird.

7. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass als Zusatzinformation eine bei jedem Prüfvorgang ändernde Laufnummer verwendet wird.

8. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass als Zusatzinformation Datum und/oder Uhrzeit verwendet wird.

9. Verfahren nach Anspruch 2, dadurch gekennzeichnet, dass als Zusatzinformation eine Zufallsinformation verwendet wird.

2802430

10. Verfahren nach einem der voranstehenden Ansprüche, dadurch gekennzeichnet, dass ein vorbestimmter Teil der permanenten Information als z.B. die Identität des Kennkartenbenutzers beinhaltende Kenninformation verwendet wird.

11. Verfahren nach einem der voranstehenden Ansprüche, dadurch gekennzeichnet, dass durch die Identifikations- oder Prüfinformation bestimmte Teile der permanenten Information als Kenninformation verwendet werden.

12. Verfahren nach einem der voranstehenden Ansprüche, dadurch gekennzeichnet, dass die permanente Information auf der Kennkarte durch die räumliche Anordnung einer Vielzahl von in die Karte eingebetteten, der mechanischen Abtastung nicht zugänglichen optischen Reflexflächen dargestellt ist und alle übrigen Informationen auf einer Magnetspur gespeichert sind.

13. Verfahren nach den Ansprüchen 3 und 12, dadurch gekennzeichnet, dass Gruppen von Reflexflächen in Reflexzonen zusammengefasst sind und dass mindestens eine dieser Reflexzonen durch die Auswahlinformation für die Chiffrierung ausgewählt wird.

14. Identifikationseinrichtung mit Kennkarten, die zwei maschinell lesbare Informationen tragen, wobei die eine Information permanent und die andere Information veränderbar gespeichert ist, und mit einer Erstellungs- und Prüfstation für die Kennkarte, welche Station erste Mittel zum Ablesen der permanenten Information, zweite Mittel zum Ablesen der veränderbar gespeicherten Information und erste Schreibmittel zum veränderbaren Speichern von Information auf den Kennkarten sowie eine mit den beiden Ablesemitteln und den ersten Schreibmitteln zusammenwirkende Auswertestufe umfasst, dadurch gekennzeichnet, dass die Auswertestufe (52) einen Speicher (17) für eine geheime Schlüsselinformation, eine Entscheidungsstufe (18) und einen Chiffriergenerator (16) enthält, welcher aus der

im Speicher (17) gespeicherten geheimen Schlüsselinformation und der von den ersten Lesemitteln (67) jeweils von den Karten abgelesenen permanenten Information eine erste Ausgangsinformation generiert, dass die Entscheidungsstufe bei der Prüfung einer Karte die erste Ausgangsinformation als Prüfinformation auf Uebereinstimmung mit der von den zweiten Lesemitteln (3) von der betreffenden Karte als Identifikationsformation abgelesen veränderbaren Informationen prüft, und dass die Schreibmittel (3) bei der Erstellung einer Karte die erste Ausgangsinformation als Identifikationsinformation auf der jeweiligen Karte speichern.

15. Einrichtung nach Anspruch 14, dadurch gekennzeichnet, dass die Auswertestufe (52) einen an den Chiffriergenerator (16) angeschlossenen Generator (26) zur Erzeugung einer sich von Prüfung zu Prüfung ändernden Zusatzinformation umfasst, dass zweite Schreibmittel zum Speichern dieser Zusatzinformation auf den Kennkarten vorgesehen sind, dass dritte Lesemittel (3) vorgesehen sind, welche die Zusatzinformation von den Kennkarten ablesen, und dass der Chiffriergenerator die erste Ausgangsinformation aus der Schlüsselinformation, der von den ersten Lesemitteln abgelesenen permanenten Information und der von den dritten Lesemitteln abgelesenen Zusatzinformation erzeugt.

16. Einrichtung nach Anspruch 15, dadurch gekennzeichnet, dass die zweiten und die ersten Schreibmittel sowie die zweiten und die dritten Lesemittel identisch sind.

17. Einrichtung nach einem der Ansprüche 14-16, dadurch gekennzeichnet, dass an den Chiffriergenerator angeschlossene Mittel (25) zur Eingabe einer Gedächtnisinformation in den Chiffriergenerator vorgesehen sind, und dass der Chiffriergenerator bei der Erzeugung der ersten Ausgangsinformation diese Gedächtnisinformation mitberücksichtigt.

18. Einrichtung nach Anspruch 15, dadurch gekennzeichnet, dass Mittel (67) zur Auswahl von Teilen der auf den Karten gespeicherten permanenten Information vorgesehen sind, dass der Chiffriergenerator aus der von den dritten Lesemitteln abgelesenen Zusatzinformation und der geheimen Schlüsselinformation eine zweite Ausgangsinformation generiert, aufgrund welcher die Auswahlmittel die Teile der permanenten Information auswählen.

19. Einrichtung nach einem der Ansprüche 15-18, dadurch gekennzeichnet, dass die Erstellungs- und Prüfungsstation eine Ein- und Ausgabestufe (32b) für Dateninformation, einen von dieser und dem Chiffriergenerator (16) angesteuerten Chiffriermischer (27), welcher die Dateninformation mittels der ersten Ausgangsinformation chiffriert, dritte Schreibmittel zum Speichern der chiffrierten Dateninformation auf den Kennkarten, vierte Lesemittel zum Ablesen der auf den Kennkarten gespeicherten chiffrierten Dateninformation, und einen von den vierten Lesemitteln und dem Chiffriergenerator angesteuerten und an die Ein- und Ausgabestufe angeschlossenen Dechiffriermischer (28) enthält, welcher die von den vierten Lesemitteln abgelesene chiffrierte Dateninformation mittels der ersten Ausgangsinformation dechiffriert und an die Ein- und Ausgabestufe weitergibt.

20. Einrichtung nach Anspruch 19, dadurch gekennzeichnet, dass die zweiten und die vierten Lesemittel sowie die ersten und die dritten Schreibmittel identisch sind.

21. Einrichtung nach Anspruch 19 oder 20, dadurch gekennzeichnet, dass die Ein- und Ausgabestufe ein Geldauszahlungsautomat mit einer Kontoführungsvorrichtung ist und Eingabemittel besitzt, mittels welcher die Höhe eines von einem durch die jeweilige Kennkarte definierten Guthabenkonto abzuhebenden Betrags eingebbar ist, dass die

Kontoführungsvorrichtung den nach einer Abhebung revidierten Kontostand als Dateninformation dem Chiffriermischer (27) zuführt und dass sie vor jeder Auszahlung den von den Kennkarten abgelesenen und vom Dechiffriermischer (28) dechiffrierten jeweiligen alten Kontostand mit der Höhe des eingegebenen abzuhebenden Betrags vergleicht und eine Auszahlung verhindert, wenn der Betrag grösser als der Kontostand ist.

22. Einrichtung nach einem der Ansprüche 14-21, dadurch gekennzeichnet, dass die Erstellungs- und Prüfstation eine Auswahlstufe (32a) aufweist, die Teile der permanenten Information als Kenninformation auswählt.

23. Einrichtung nach einem der Ansprüche 14-22, dadurch gekennzeichnet, dass die Erstellung- und Prüfstation einen Löschkopf (11) und Positioniermittel (32a) für den Löschkopf besitzt, die bei jeder Prüfung einer Kennkarte ausgewählte Teile der permanent gespeicherten Karteninformation irreversibel löschen.

DR. BERG DIPL.-ING. STAPF
DIPL.-ING.
8 MÜNCHEN 60 · ZUGSPITZSTR. 45

2802430

GRETAG AKTIENGESELLSCHAFT, 8105 Regensdorf/ZH (Schweiz)

Case 7-10945/GTS 423/K/K

Deutschland

Anwaltsakte 28 788 20. Januar 1978

Identifikationsverfahren und -einrichtung

Die Erfindung betrifft ein Identifikationsverfahren unter Verwendung einer zwei maschinell lesbare Informationen tragenden Kennkarte, auf der eine Information permanent und die andere Information veränderbar gespeichert ist.

Identifizierungskarten werden verwendet zur maschinellen Personenidentifikation,

als Kreditkarten, als Personalausweis oder zum Geld-Abheben bei Geldauszahlungs-Automaten und dergleichen. Meist wird dabei in einer Prüfstation während eines Prüfvorganges die Echtheit der Identifizierungskarte überprüft.

Von einer guten Identifizierungskarte wird eine hohe Fälschungssicherheit, das heisst Sicherheit gegen das Kopieren durch Unberechtigte verlangt, um zum Beispiel den Raumzutritt durch Unberechtigte oder das unbefugte Geldabheben zu verhindern. In bekannten Systemen wird die Fälschungssicherheit oft dadurch erzielt, dass Identifizierungskarten schwierig und nur mit kostspieligen Einrichtungen herstellbar sind, welche nur bei der Massenfertigung der Karten wirtschaftlich sind und Kopien von einzelnen Karten viel zu teuer zu stehen kommen. Meist ist bei diesen Systemen die in den Identifizierungskarten gespeicherte Information nicht änderbar. Dies bringt die zwei folgenden Nachteile mit sich. Erstens muss eine Benützer-Organisation des Identifizierungssystems die Karten schon fertig codiert vom Hersteller beziehen und kann sie selbst nicht umcodieren. Dies beeinträchtigt die Geheimhaltung wesentlich. Zweitens sind variable Daten auf den Identifizierungskarten wie der Kontosstand eines Geldbezugskontos oder der Zeit-Saldo bei Gleitzeitsystemen auf der Identifizierungskarte nicht speicherbar.

Bei einem weiteren bekannten System ist die Karteninformation in einer Magnetspur leicht beschreibbar, lesbar und löschbar enthalten. Eine Umcodierung durch die Benützer-Organisation ist leicht möglich, jedoch ist die Fälschungssicherheit der Karte für sich allein sehr gering. Sie wird dadurch erhöht, dass für die Identifikation zusätzlich zur Karteninformation während des Prüfvorganges durch den Kartenbesitzer eine individuelle, geheime Kennzahl in die Tastatur der Prüfstation

auf Korrespondenz mit der Karteninformation überprüft wird.

Die Nachteile hier sind, dass einerseits das System nur fälschungssicher ist, solange die geheime Kennzahl nicht verraten ist, und ferner, dass bei jeder Identifikation diese Kennzahl einzutasten ist.

Bei einem weiteren bekannten Verfahren zur Erzielung von guter Fälschungssicherheit von Identifizierungskarten, wie beispielsweise im CH-Patent 554 574 beschrieben, wird auf einer konventionellen beschreib- und löschbaren Informationsspur der Identifizierungskarte, also zum Beispiel einer Magnetspur, die leicht variierbare Hauptinformation gespeichert und in einem anderen Kartenteil wird die schwer fälschbare, feste und individuelle Identifikations-Information in einer anderen, schwer kopierbaren Speicherungsart gespeichert. Diese Identifikationsinformation wird zusätzlich in der Magnetspur gespeichert und während des Prüfvorgangs auf Uebereinstimmung mit der schwer fälschbaren Information überprüft. Obwohl die zusätzliche Speicherung der individuellen Identifikationsinformation in anderer Codierung als die der schwer fälschbaren Information erfolgen oder in die Hauptinformation eingeschachtelt sein kann, besteht doch eine feste und erkennbare Korrespondenz zwischen der in der Informationsspur und der in der schwer kopierbaren Speicherungsart gespeicherten Information, und die Fälschungssicherheit ist nur bedingt gewährleistet.

Die Erfindung hat zum Ziel, alle diese Nachteile zu vermeiden. Es werden Identifizierungskarten mit den beiden Speicherarten einerseits Magnetspur mit leicht

variierbarer Information und andererseits eine schwer kopierbare, fälschungssichere Speicherart für mehrheitliche feste Information verwendet.

Die fälschungssichere Information oder ausgewählte Teile davon beeinflussen die leicht variierbare Information mittels kryptotechnischer Methoden, sodass eine Korrespondenz der beiden Informationen nicht erkennbar ist und die leicht variierbare Information ebenso fälschungssicher wird wie die schwer kopierbare Information.

Durch kryptotechnische Auswahl von kleinen Teilen der fälschungssicheren Information ist die Fälschungssicherheit ebenso gross wie bei Verwendung der gesamten fälschungssicheren Information.

Das erfindungsgemässe Verfahren ist gekennzeichnet dadurch, dass die veränderbare, im folgenden Identifikationsinformation genannte Information bei der Erstellung der Karte durch Chiffrierung aus zumindest ausgewählten Teilen der auf der Karte vorhandenen permanenten Information und einer geheimen Schlüsselinformation gebildet und auf der Karte gespeichert wird, und dass bei der Prüfung der Karte aus denselben ausgewählten Teilen der permanenten Information und der geheimen Schlüsselinformation eine Prüfinformation gebildet und auf Uebereinstimmung mit der auf der Karte gespeicherten Identifikationsinformation geprüft wird.

In einer besonders wirksamen Variante des Verfahrens wird die Art der Chiffrierung bei jedem neuen Prüfvorgang geändert, derart, dass keine Korrespondenz der beiden verschiedenartig auf der Identifizierungskarte gespeicherten Informationen erkennbar ist.

Im folgenden wir die Erfindung anhand der in den Figuren gezeigten Ausführungsbeispiele näher erläutert. Es zeigen:

Fig. 1a und 1b ein Prinzipschema einer Identifizierungskarte in perspektivischer Darstellung (1a) und in Aufsicht (1b),

Fig. 2 eine prinzipielle Anordnung zur Durchführung des Verfahrens,

Fig. 3 einen vergrösserten Teilausschnitt aus Figur 2,

Fig. 4 einen Schnitt gemäss der Schnittlinie IV - IV aus Figur 3,

Fig. 5 eine untere Hälfte aus Figur 4,

Fig. 6 ein Detail aus Figur 4 mit einer Abtasteinrichtung,

Fig. 7 und 8 ein weiteres Ausführungsbeispiel in Aufriss und Grundriss und

Fig. 9 ein detailliertes Ausführungsbeispiel zur Durchführung des Verfahrens.

Auf einer Identifizierungskarte 1, im Ausführungsbeispiel als CREDIT CARD dargestellt, ist eine Magnetspur 2, mittels einem Magnetkopf 3, abtastbar, schreib- und löschbar aufgebracht. Ferner erhält die Karte ein Feld RF mit einer Anzahl Speicher-

stellen RZ, welche fälschungssichere Information IU enthalten. Diese letztere Information ist mit einem Abtastkopf 67 abtastbar.

Im Blockschema der Figur 2 ist eine Identifizierungskarte zur Durchführung des erfindungsgemässen Verfahrens schematisiert gezeichnet, wobei in diesem Ausführungsbeispiel die Speicherstellen RZ in Zeilen und Kolonnen eines X-Y-Koordinatensystems angeordnet sind. Es sind, als Beispiel, zehn Zeilen Y_1 bis Y_{10} und zwanzig Kolonnen X_1 bis X_{20} von Speicherstellen RZ vorhanden, also total 200 Speicherstellen. Jede Speicherstelle kann z.B. 10^6 bit Information enthalten, wobei dann die gesamte fälschungssichere Information der Karte nach diesem Ausführungsbeispiel $2 \cdot 10^8$ bit betragen würde. Die Speicherstellen RZ können gemäss der Figuren 3 bis 5 ausgeführt sein. Der Abtastkopf 67 für die Abtastung der Speicherstellen RZ kann mit einer Steuerinformation IS über eine Leitung 50 so gesteuert werden, dass die Information jeder einzelnen Speicherstelle abtastbar ist.

Der Abtastkopf kann z.B. in Y-Richtung, mittels Schrittmotor angetrieben zur Zeilen-Auswahl beweglich sein, während die Kolonnenauswahl durch ein Zeitfenster während des Kartendurchlaufs durch die Prüfstation in X-Richtung erfolgt. Sowohl Zeilen- als auch Kolonnenauswahl wird durch die Steuerinformation IS gesteuert.

In Figur 2 sind sämtliche Informationsflüsse mit Pfeilen markiert.

An einem in einer Prüfstation 52 vorgesehenen Chiffrierrechner 16 stehen als Eingangsinformationen mindestens die einem Geheimschlüsselspeicher 17 entnommene Geheimschlüsselinformation IE_1 sowie mindestens Teile der fälschungssicheren Information IU als Eingangsinformation IE_2 zur Verfügung.

Mit diesen Eingangsinformationen wird die Ausgangsinformation IA_1 errechnet, welche direkt oder indirekt über eine Mischer- und Vergleicher-Schaltung 18 als magnetische Information IM mittels des Magnetkopfes 3 auf der Magnetspur 2 gespeichert wird. Infolge der Chiffrierung ist es praktisch unmöglich, aus der magnetisch gespeicherten Information IM Rückschlüsse auf die fälschungssichere Information IU zu ziehen.

Solche Rückschlüsse sind aber vollends unmöglich, wenn als zusätzliche Eingangsinformation IE_3 eine variable Information IV , erzeugt in einem Generator 26, in den Chiffrierrechner 16 eingegeben wird. Die variable Information ändert sich bei jedem Prüfvorgang, sodass die im Chiffrierrechner 16 errechnete Ausgangsinformation IA_1 und damit auch die magnetisch gespeicherte Information IM nach jedem Prüfvorgang wieder anders ist. Die variable Information IV wird in einer Schreibphase des Prüfvorganges einerseits in den Chiffrierrechner als Information IE_3 eingegeben, wo sie die Ausgangsinformation IA_1 mitbestimmt, welche letztere auf der Magnetspur geschrieben wird. Andererseits wird die variable Information IV über eine Leitung 51 und eine weitere Leitung 8 direkt auf die Magnetspur geschrieben. Beim nächsten Prüfvorgang wird sie dann in der Lese- und Prüfphase mit dem Magnetkopf 3 ausgelesen und als Eingangsinformation IE_3 des Chiffrierrechners 16 zur Bildung der Ausgangsinformation IA_1 verwendet.

Diese Vorgänge werden weiter unten anhand von Fig.9 im einzelnen beschrieben.

Die variable Information (IV) kann eine fortlaufende Laufnummer sein, welche im Generator 26 erzeugt wird und bei jedem Prüfvorgang einen neuen Wert annimmt.

Die variable Information IV kann auch eine Datum-Uhrzeit-Information sein, welche dann einer elektronischen Uhr des Generators 26 entnommen wird.

Im weiteren kann die variable Information IV eine Zufallszahl sein, welche dann in einem Rausch- oder Zufallsgenerator oder einem Pseudo-Zufallsgenerator des Generators 26 entnommen wird.

Jede einzelne Identifizierungskarte kann von allen andern abweichende fälschungssichere Information enthalten.

Damit wird ein sehr hoher Sicherheitsgrad erreicht, da in diesem Fall ein Fälscher für jede einzelne Identifizierungskarte einer Organisation den sehr grossen Aufwand für das Kopieren aufbringen müsste.

Für geringere Sicherheitsanforderungen kann jedoch die fälschungssichere Information mit Ausnahme der Karten-Nummer für alle Identifizierungskarten die gleiche sein, wodurch die Kosten für die Kartenherstellung etwas reduziert sind. Die Sicherheit wird durch die pseudozufällige Auswahl bestimmter Teile der fälschungssicheren Information mittels Chiffrierrechner gewährleistet.

Ein Teil der fälschungssicheren Information IU kann eine Kenninformation ID_U, das heisst, beispielsweise eine codierte Karten-Nummer sein, welche von Karte zu Karte verschieden ist. Diese Information kann in der Prüfstation 52 in einem Steuerteil 32 überprüft werden.

Diese Kenninformation könnte zum Beispiel aus der Information einer einzigen der 200 Speicherstellen RZ mit 10^6 bit bestehen, also beispielsweise die Speicherstelle im Kreuzpunkt X_7, Y_5 von Figur 2.

Zur Erhöhung der Fälschungssicherheit könnte zu dieser festen Kenninformation ID_U eine mit dem Abtastkopf 67 aus dem Speicherfeld RF ausgewählte Information als zusätzliche Kenninformation verwendet werden, wobei die Steuerinformation IS für diese Auswahl eine Ausgangsinformation IA_2 des Chiffrierrechners 16 sein würde, welche mit der festen Kenninformation ID_U als Eingangsinformation IE_2 des Chiffrierrechners 16 gewonnen würde.

Ein Fälscher müsste also nicht nur eine einzige Speicherstelle RZ, sondern die ganze Karte kopieren, da er nicht weiss, welche Speicherstelle durch den Chiffrierrechner ausgewählt wird.

Auf der Identifizierungskarte 1 kann weit mehr fälschungssichere Information, nämlich zum Beispiel $2 \cdot 10^8$ bit, aufgebracht sein, als in nützlicher Frist verarbeitbar ist. Trotzdem kann die volle Sicherheit, welche die grosse, ganze Informationsmenge bietet, ausgenützt werden. Es kann zum Beispiel mit der variablen Information IV als Eingangsinformation IE_3 des Chiffrierrechners 16, natürlich zusammen mit der Geheimschlüsselinformation IE_1 eine Ausgangsinformation IA_2

errechnet werden, welche durch Steuerung des Abtastkopfes auf einer der 200 Speicherstellen RZ eine Teilinformation der fälschungssicheren Information IU auswählt und als neue Eingangsinformation IE_2 des Chiffrierrechners zur Berechnung der Ausgangsinformation IA_1 zur Verfügung stellt. Diese Teilinformation kann zum Beispiel nur der Inhalt einer einzigen, auf diese Art pseudozufällig ausgewählten Speicherstelle RZ sein, d.h. hier etwa 0,5% der gesamten fälschungssicheren Information.

Man hat nur die Information einer einzigen Speicherstelle RZ abzutasten und zu verarbeiten und trotzdem ist die Fälschungssicherheit so gross, wie wenn alle 200 Speicherstellen berücksichtigt würden, da der Fälscher ja nicht weiss, welche Speicherstelle vom Chiffrierrechner "zufällig" selektioniert wird.

Figur 3 stellt einen vergrösserten Teilausschnitt aus der Identifikationskarte 1 mit lediglich zwei teilweise skizzierten Reflexzonen RZ dar. Diese Reflexzonen RZ bestehen aus einer Reihe von Grenzflächen R_n, die über die Breite B der Zonen verlaufen und sind gegeneinander durch Begrenzungskanten K abgetrennt. Zwischen den einzelnen Reflexzonen RZ sind sogenannte Trennzonen TZ vorgesehen. Die Abmessung einer Grenzfläche R_n in Richtung des Pfeiles L kann beispielsweise 0,2 mm betragen, die Breite B quer dazu ca. 2 mm, sodass die Reflexzone mit 10 Grenzflächen ein Quadrat von 2 x 2 mm^2 bildet.

Beim in Figur 4 dargestellten Schnitt durch die Identifizierungskarte ist gezeigt, dass die Karte im wesentlichen aus einer aus Kunststoff hergestellten oberen Kartenschicht 1b und aus einer in ähnlichem Material hergestellten unteren

Kartenschicht 1a . besteht. Letztere ist dabei Träger der Grenzflächen R mit entsprechenden Begrenzungskanten K, die die Reflexzonen RZ bilden und durch Trennzonen TZ voneinander getrennt sind. Die untere Kartenschicht 1a trägt auf ihrer Unterseite eine Magnetspurschicht 2. Die beiden Kartenschichten sind fest miteinander verbunden. Die obere Kartenschicht 1b muss somit entweder ein Negativ der unteren Kartenschicht 1a sein, oder sie muss in plastischem oder flüssigem Zustand auf die untere Kartenschicht 1a aufgebracht werden, ohne allerdings die Grenzflächen R zu verändern.
Die Verbindung kann beispielsweise durch thermisches Ultraschall-Schweissen bei den Trennzonen TZ, oder durch Verkleben der ganzen Kartenfläche erfolgen. Die Verbindung der beiden Kartenschichten muss in jedem Fall so beschaffen sein, dass eine nachträgliche Trennung ohne Beschädigung der Grenzflächen weder mechanisch noch mit Lösungsmitteln realisiert werden kann.

Figur 5 zeigt einen Schnitt gemäss Schnittlinie V - V durch die untere Kartenschicht 1a (die obere Kartenschicht 1b wurde in dieser Figur der Uebersichtlichkeithalber nicht dargestellt), die,wie schon erwähnt, in Reflexzonen RZ und Trennzonen TZ unterteilt ist. Die Reflexzonen wiederum sind mit einer Anzahl Grenzflächen $R_1 \ldots\ldots R_n$ bestückt, welche bezüglich der Kartenebene verschiedene Winkelstellungen, α_2, α_4, α_5 und α_{n-1} aufweisen. Die Anordnung der Grenzflächen R ist üblicherweise von Reflexzone zu Reflexzone verschieden. Im skizzierten Ausführungsbeispiel sind pro Reflexzone 10 Grenzflächen mit je 4 möglichen Winkelstellungen vorgesehen, was bedeutet, dass $4^{10} \approx 10^6$ voneinander verschiedene Reflexzonen möglich sind. Natürlich kann die Anzahl der Grenzflächen pro Reflexzone sowie auch die Anzahl der verschiedenen Grenzflächen von diesem Aus-

führungsbeispiel abweichen. Die Reflexzonen RZ mit den Grundflächen R können mit je einem Prägestempel durch Einpressen in den Kunststoff in plastischem Zustand oder in einem Kunststoff-Spritzvorgang hergestellt sein. Im Ausführungsbeispiel ist die obere Seite der unteren Kartenschicht metallisiert, zum Beispiel durch Aufdampfung oder galvanisch, sodass die Grenzflächen R mit einer das Licht reflektierenden Metallschicht 1c versehen sind. Im Raum der Trennzonen TZ ist die Metallschicht abgetragen, sodass in diesen Zonen eine Kunststoffschicht 1d zur Verfügung steht und damit eine gute Verbindung zwischen den beiden Karten sichergestellt.

In Figur 6 ist ein Ausführungsbeispiel einer optischen Abtasteinrichtung der Identifizierungskarte schematisch dargestellt. Die optische Abtasteinrichtung sowie auch der Schreib- und Lesekopf 3 für die Abtastung der Magnetspur sind in der Prüfstation eingebaut, welche die Identifizierungskarte 1 zur Prüfung in Pfeilrichtung L durchläuft. Eine Lichtquelle 5, zum Beispiel ein LASER-Generator, liefert einen feinen Lichtstrahl 5a, welcher auf die Identifizierungskarte fällt und von den Grenzflächen R_1 bis R_{10} reflektiert wird. Diese Grenzflächen können beispielsweise vier verschiedene Winkelstellungen α (Fig. 5) aufweisen und der reflektierte Lichtstrahl 5b kann zum Einfalls-Lichtstrahl vier verschiedene Winkel γ_1 bis γ_4 aufweisen. Für jede dieser vier Richtungswinkel ist eine Photodiode P_1 bis P_4 vorhanden. In der in Figur 6 gezeichneten Kartenposition trifft der Lichtstrahl 5a auf die reflektierende Grenzfläche R_4 und wird als reflektierter Strahl 5b auf die Photodiode P_2 geworfen, welche einen Photostrom an die Verteilerschaltung 7 abgibt. Beim Durchlauf der Reflexzone RZ von Figur 6 unter dem Abtast-Lichtstrahl 5a, werden, entsprechend den Winkelstellungen der Grenzflächen R_1 bis R_{10}, durch die vier Photodioden P_1 bis P_4 in Sequenz zehn Photostrom-Signale an die Verteiler-

schaltung 7 abgegeben, welche in dieser verstärkt werden und beispielsweise binär codiert mit je einer verschiedenen 3-bit-Zahl pro Photodiode an den Ausgang 10 der Schaltung 7 gelangen.

Der Zählbeginn für die zehn Photostrom-Signale wird durch den Uebergang des Abtast-Lichtstrahls 5a von der Trennzone TZ, wo kein Photostrom fliesst, auf die erste Grenzfläche festgelegt. Die Kanten der Trennzonen sind diffus reflektierend.

Die vier Photodioden P_1 bis P_4 mit der Lichtquelle 5 bilden zusammen das Photo-Abtastsystem 6, welches auch quer zur Kartenlaufrichtung verstellbar ist, um sämtliche der flächenhaft angeordneten Reflexzonen abtasten zu können, wie schon oben beschrieben wurde. Das Photo-Abtastsystem 6 mit der Verteilerschaltung 7 bilden zusammen den Abtastkopf 67, welcher die Speicherstellen RZ der fälschungssicheren Information IU abtastet.

Bei der Verwendung der Identifizierungskarte für die Geldausgabe mittels "Off-Line" arbeitenden Geldausgabeautomaten, wobei der aktuelle Kontostand chiffriert auf der Identifizierungskarte festgehalten ist, besteht für den befugten Karteninhaber, welcher eine echte und individuelle Identifizierungskarte besitzt und auch mit seiner idividuellen Gedächtnis-Kennzahl arbeitet, trotz all den beschriebenen, fälschungssicheren Methoden die Möglichkeit des Betruges.

Der befugte Karteninhaber muss hierzu nur die magnetisch gespeicherte Information welche unter anderem auch den aktuellen Kontostand enthält, vor dem Geldabheben auf ein Tonband kopieren, dann Geld an einem der Automaten abheben, wobei gleich-

zeitig der neue, reduzierte Kontostand chiffriert in die Magnetspur geschrieben wird. Diese Information kann er dann mit der Tonbandkopie, welche noch dem höheren Kontostand entspricht, überschreiben und an einem zweiten Automaten Geld abheben und so fort.

Natürlich könnte man dies verhindern, wenn ein Kontobetrag nur an einem ganz bestimmten Automaten bezogen werden müsste, wobei diese Automaten-Nummer als weitere Eingangsinformation des Chiffrierrechners wirken würde. Oder man könnte zwischen zwei Abhebungen mittels der elektronischen Uhr, welche die Datum-Zeit-Information als variable Information liefert, eine Zeitsperre einschalten, bis der Kontostand allen Off-Line arbeitenden Geldausgabeautomaten mitgeteilt ist.

All dies ist aber umständlich und es wird daher vorgeschlagen, nach jeder einzelnen Kartenprüfung mindestens eine der Reflexzonen irreversibel zu löschen, um eine fälschungssichere Kontrolle über die Anzahl der Kartenprüfungen zu erhalten.

Dies kann, gemäss den Figuren 7 und 8 dadurch geschehen, dass im Kartenmaterial eine thermisch schwärzbare Substanz, wie sie vom Thermodruck her bekannt ist, enthalten ist. Angesteuert durch einen Eingang 13 wird in einem Löschkopf 11 einer Heizspule 12 ein Stift 11a erwärmt, welcher die darunter liegende Reflexzone schwärzt und damit auslöscht.

Durch die Steuerung des Eingangs 13 kann der Löschkopf 11 auf jede gewünschte Reflexzone gestellt werden.

Die Auslöschung von einzelnen Reflexzonen kann auch durch Ausstanzen erfolgen, wobei der Löschkopf 11 durch einen Stanzkopf zu ersetzen ist.

Die Prüfung der gelöschten Reflexzonen erfolgt ebenfalls mit dem Abtastkopf 67. Bei 200 Reflexzonen könnten zum Beispiel 100 gelöscht werden, das heisst 100 Kartenprüfungen vorgenommen werden, bis die Identifizierungskarte zu ersetzen ist.

Gemäss Figur 9 erfolgt das irreversible Löschen von Speicherstellen beziehungsweise Reflexzonen RZ der fälschungssicheren Information mit dem Löschkopf 11, beginnend in der untersten Zeile Y_1, wobei, gesteuert durch eine erste Station 32a des Steuerteiles 32 mit Information IL über den Eingang 13 bei jedem Prüfvorgang eine Speicherstelle RZ gelöscht wird. Der Löschkopf 11 steht auf der Speicherstelle X_9 der Zeile Y_1.

Der Abtastkopf 67 wird bei jedem Prüfvorgang, gesteuert durch die erste Station 32a, die Zeile mit den gelöschten Speicherstellen abtasten und als weitere Eingangsinformation in den Chiffrierrechner eingeben. Auf diese Weise wird die oben beschriebene Betrugsmöglichkeit ausgeschlossen, da die alte Magnetspur mit der neuen zu löschenden Information nicht übereinstimmt.

Beim erfindungsgemässen Verfahren liegt ein wesentlicher Teil der Sicherheit

gegen Fälschungen darin, dass die Auswahl der fälschungssicheren Information durch einen Geheimschlüssel mit Chiffrierrechner bestimmt ist.

Diese Auswahl kann einerseits durch die variable Invormation IV und andererseits durch Auswechseln des Geheimschlüssels leicht geändert werden.

Die Sicherheit gegen Fehlabtastungen der Identifizierungskarten kann durch die bekannten Redundanzmethoden wie Mehrfach-Speicherung, fehlererkennende oder fehlerkorriegierende Codes, usw. gewährleistet werden. Eine Fehlabtastung der optisch abtastbaren fälschungssicheren Information durch Verschmutzung einer Reflexzone RZ kann dadurch unwirksam gemacht werden, dass es zugelassen ist, die Karte mehrmals abtasten zu lassen, wobei bei jeder neuen Abtastung durch Wirkung der variablen Information eine neue Reflexzone RZ durch den Chiffrierrechner ausgewählt wird.

Anhand von Figur 9 soll nun erläutert werden, wie die Identifikation sowie die fälschungssichere Speicherung von variablen Daten, zum Beispiel Geldbeträgen oder Zeit-Saldi vor sich gehen kann. Es wird hier nur ein Beispiel beschrieben, aber die Erfindung beschränkt sich keineswegs darauf.

Das Beispiel bezieht sich auf sehr hohe Fälschungssicherheit,und in vielen praktischen Fällen können einzelne der beschriebenen Massnahmen weggelassen werden.

Für die Identifikation besteht ein Prüfvorgang aus einer Identifikationsphase und einer daran anschliessenden Eingabephase. Obwohl der Prüfvorgang jeweils mit der Identifikationsphase beginnt, wird zuerst die Eingabephase beschrieben.

2802430

Ein Selektionierschalter 30 ist durch die erste Station 32a mittels Information IC in Stellung a gestellt. Auf den Chiffrierrechner 16 werden, ausser der immer vorhandenen Geheimschlüsselinformation IE_1, eingegeben:

- die Eingangsinformation (IE_3) aus dem Generator 26 für die variable Information IV
- die geheime, individuelle Kennzahl oder Gedächtniszahl aus einer Tastatur 25.

Die variable Information IV wird als magnetische Information IM durch einen Schreibkopf 3a des Magnetkopfes auf die Magnetspur geschrieben. Die Information IO aus der ersten Station 32a bewirkt als den Abtaskopf 67 steuernde Information IS, dass von diesem die Identifikations-Information ID_U als Teil der fälschungssicheren Information IU (also zum Beispiel Reflexzone RZ mit Kreuzungspunkt X_1, Y_2 im Feld RF der fälschungssicheren Informationen) abgelesen und einerseits in die erste Station 32a und andererseits als Eingangsinformation IE_2 auf den Chiffrierrechner 16 gelangt, in welchem zusammen mit den übrigen Eingangsinformationen eine Ausgangs-Information IA_2 errechnet wird, welche in Stellung b des Sektionsschalters 30 als Steuerinformation den Abtastkopf 67 neu und pseudozufällig positioniert. Der Drehschalter 30 wird in Stellung c gebracht und die vom Abtastkopf 67 gelesene Teilinformation gelangt einerseits als weitere Identifizierungsinformation ID_U auf die erste Station 32a und andererseits als weitere Eingangsinformation IE_2 auf den Chiffrierrechner, in welchem die Ausgangsinformatic IA_1 errechnet und als magnetische Information IM auf die Magnetspur geschrieben wird.

In der Identifikationsphase ist die Schalterstellung des Selektionsschalters 30 zu Beginn ebenfalls auf a. Mittels der Tastatur 25 wird die individuelle Kenn-

zahl als Eingangsinformation IE_4 in den Chiffrierrechner 16 eingegeben. Von der Magnetspur 2 wird mittels eines Lesekopfes 3b des Magnetkopfes die beim vorhergehenden Prüfvorgang geschriebene variable Information als magnetische Information IM_b ausgelesen und als Eingangsinformation IE_3 in den Chiffrierrechner gegeben. Die übrigen Vorgänge bis zur Erzeugung der Ausgangsinformation IA_1 sind die gleichen wie in der Eingabephase. Alsdann wird in Stellung c des Selektionsschalters 30 die beim vorhergehenden Prüfvorgang magnetisch gespeicherte Ausgangsinformation IM_b ausgelesen, auf eine Leitung 46 gegeben und in einem Vergleicher 29 mit der während der Identifikationsphase im Chiffrierrechner erzeugten Ausgangsinformation IA_1 verglichen. Das Resultat des Vergleichs heisst Identität oder Nicht-Identität und wird als Information ID_3 bei einem Punkt 22 ausgegeben. Ist Identität vorhanden und ist auch die Identifizierungs-Information ID_U in der ersten Station 32a als richtig erkannt worden, so wird auch die Identifikation als richtig taxiert. In der ersten Station 32a sind die Identifizierungs-Informationen ID_U, welche aus einem festen Teil und einem pseudozufällig ausgewählten Teil der fälschungssicheren Information IU bestehen, für alle Kartenbesitzer der Organisation gespeichert für den Vergleich.

Die fälschungssichere Speicherung und Veränderung variabler Daten, wie Geldbeträge oder dergleichen, auf der Identifizierungskarte erfolgt normalerweise im Anschluss an die Identifikationsvorgänge des Prüfvorgangs, und weist ebenfalls zwei Phasen auf. Während einer Schreibphase, welche im Anschluss an die Eingabephase erfolgt, wird in Stellung d des Selektionierschalters 30 zum Beispiel der momentane Kontostand als digitale Daten aus einer zweiten Station 32b des Steuerteils 32 in Form eines Ein-Ausgabegerätes als Information ID_1 an den Chiffrier-

mischer 27 bekannter Art abgegeben und in diesem mit den nach den oben beschriebenen Methoden entstandenen Ausgangsinformationen IA_1 zum Chiffrat gemischt und über eine Leitung 48 als magnetische Information IM_a dem magnetischen Schreibkopf 3a zugeführt und als chiffrierter Kontostand auf die Magnetspur geschrieben.

Während einer Lesephase des Prüfvorgangs, welche im Anschluss an die Identifikationsphase erfolgt, wird in Stellung d des Selektionierschalters 30 der beim vorhergehenden Prüfvorgang geschriebene, chiffrierte Kontostand von der Magnetspur abgelesen und als magnetische Information IM_b über eine Leitung 44 einem Dechiffriermischer 28 zugeführt und in diesem mit der nach der oben beschriebenen Methode entstandenen Ausgangsinformation IA_1 dechiffriert und der zweiten Station 32b als Kontostand im Klartext zugeführt. Dieser Kontostand kann auch durch Vorsetzen einer Anzahl Nullen in der zweiten Station 32b auf Authentizität überprüft werden.

Die Authentizität des Kontostandes kann auch, wie beispielsweise in der DT-OS 23 50 418 beschrieben, dadurch gewährleistet werden, dass der Kontostand einerseits als Eingangsinformation des Chiffrierrechners 16 dient und andererseits auf der Magnetspur "klar" gespeichert wird. In diesem Fall wird eine im Chiffrierrechner mittels der Eingangsinformationen

- Geheimschlüsselinformation IE_1
- fälschungssichere Information IE_2
- variable Information IV
- Kontostand ID_1

erzeugte Ausgangsinformation IA_1 als Kryptonummer samt dem Kontostand ID_1

fälschungssicheren Informationen vorhanden sein, welche während des Kartendurchlaufs durch die Prüfstation simultan mit der Magnetspur abtastbar ist. Ferner könnte die mit Chiffrierrechner, mittels Geheimschlüssel- und variabler Information selektionierte fälschungssichere Information als Chiffrierrechner-Eingangsinformation direkt die Ausgangsinformation IA mitbestimmen.

Um Fehler bei der Kartenabtastung zu eliminieren, können die fälschungssicheren Informationen in redundanten, fehlerkorrigierenden Codes bekannter Art gespeichert sein. Beispielsweise könnte jede Speicherstelle RZ über die Karte verteilt dreimal vorhanden sein und von den drei Ablesungen die zwei identischen als die richtigen ausgewählt werden.

Weiter könnte es bei Verwendung der variablen Information zulässig sein, bei einem zum Beispiel wegen Kartenverschmutzung nicht erfolgreichen Prüfvorgang weitere Prüfvorgänge durchzuführen, wobei durch die pseudozufällige Auswahl der fälschungssicheren Information auf einwandfrei lesbare Speicherstellen umgeschaltet würde.

Die ganzen Steuervorgänge sowie die Chiffrierung könnten mittels einem oder mehreren Mikroprozessoren durchgeführt werden, wodurch zufolge der relativ langsamen Abläufe all die Vorgänge in Sequenz durchgeführt würden und der Steuerungsaufwand auch für die Prüfvorgänge für höhere Sicherheit relativ klein wäre.

auf der Magnetspur 2 der Identifizierungskarte während der Schreibphase gespeichert. Während der späteren Ueberprüfung der Authentizität des Kontostandes während einer Lesephase werden die eben aufgeführten Informationen in den Chiffrierrechner eingegeben und die so entstehende Ausgangsinformation mit der gespeicherten Kryptonummer auf Uebereinstimmung überprüft.

Zum Geldabheben an einem Geldausgabe-Automaten wird alsdann mittels der Tastatur 25 ein Geldbetrag eingetastet, welcher vom Automaten ausbezahlt wird und welcher in der zweiten Station 32b vom momentanen Kontostand abgezogen wird, und wobei in der Schreibphase der neue chiffrierte Kontostand auf der Magnetspur festgehalten wird.

Eine Fälschung des chiffriert gespeicherten Kontostandes ist nicht möglich, da die Chiffrierung abhängig ist vom Geheimschlüssel sowie auch von den fälschungssicheren Karteninformationen.

Sämtliche beschriebenen Vorgänge erfolgen digital und elektronisch.

Die Leitungspunkte 8, 9, 10, 19, 20, 50 korrespondieren mit denjenigen des vereinfachten Blockschemas von Figur 2. Die erste Station 32a steuert mit der Steuerinformation IST alle nicht weiter beschriebenen Vorgänge in der Prüfstation.

Wie erwähnt, gelten die beschriebenen Vorgänge für sehr hohe Sicherheitsansprüche und können für viele Anwendungen wesentlich reduziert werden. So können für geringere Sicherheits-Anforderungen die fälschungssicheren Informationen überhaupt weggelassen, beziehungsweise nur eine Kartennummer vorhanden sein und die Karteninformation in der Magnetspur enthalten sein. Bei etwas höheren Ansprüchen könnte zum Beispiel nur eine einzige Spur, zum Beispiel die Zeile Y_1 von Figur 2, von

Leerseite

2802430

GRETAG AKTIENGESELLSCH

-35-

Nummer: 28 02 430
Int. Cl.²: G 07 C 9/00
Anmeldetag: 20. Januar 1978
Offenlegungstag: 27. Juli 1978

Fig.1a

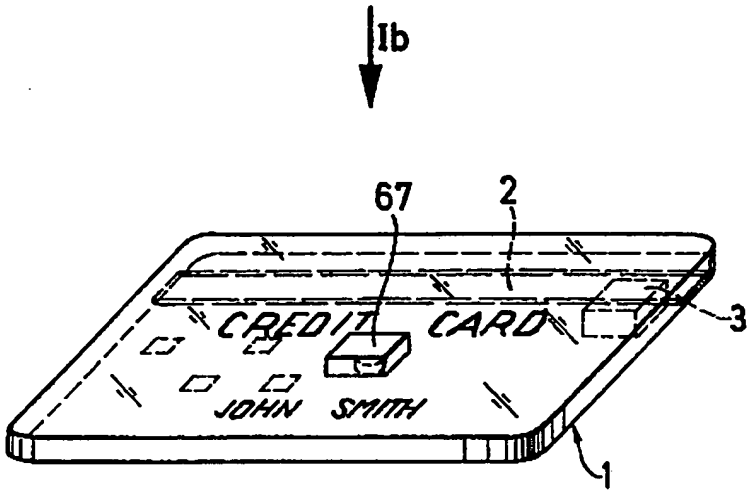


Fig. 1b

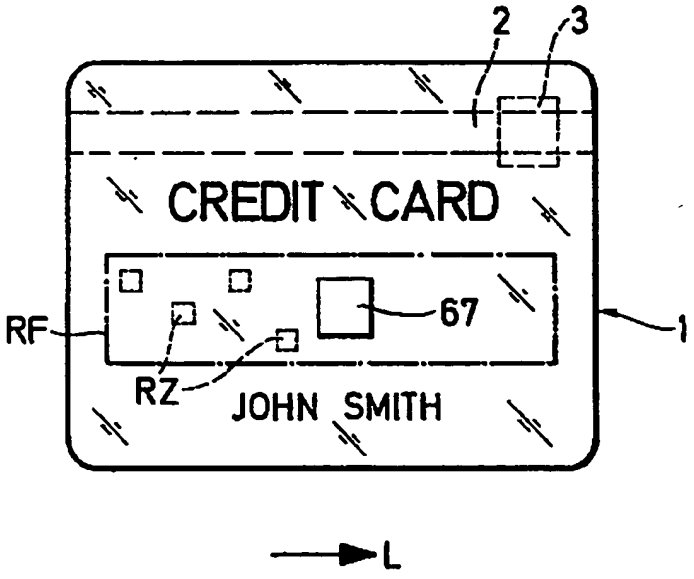
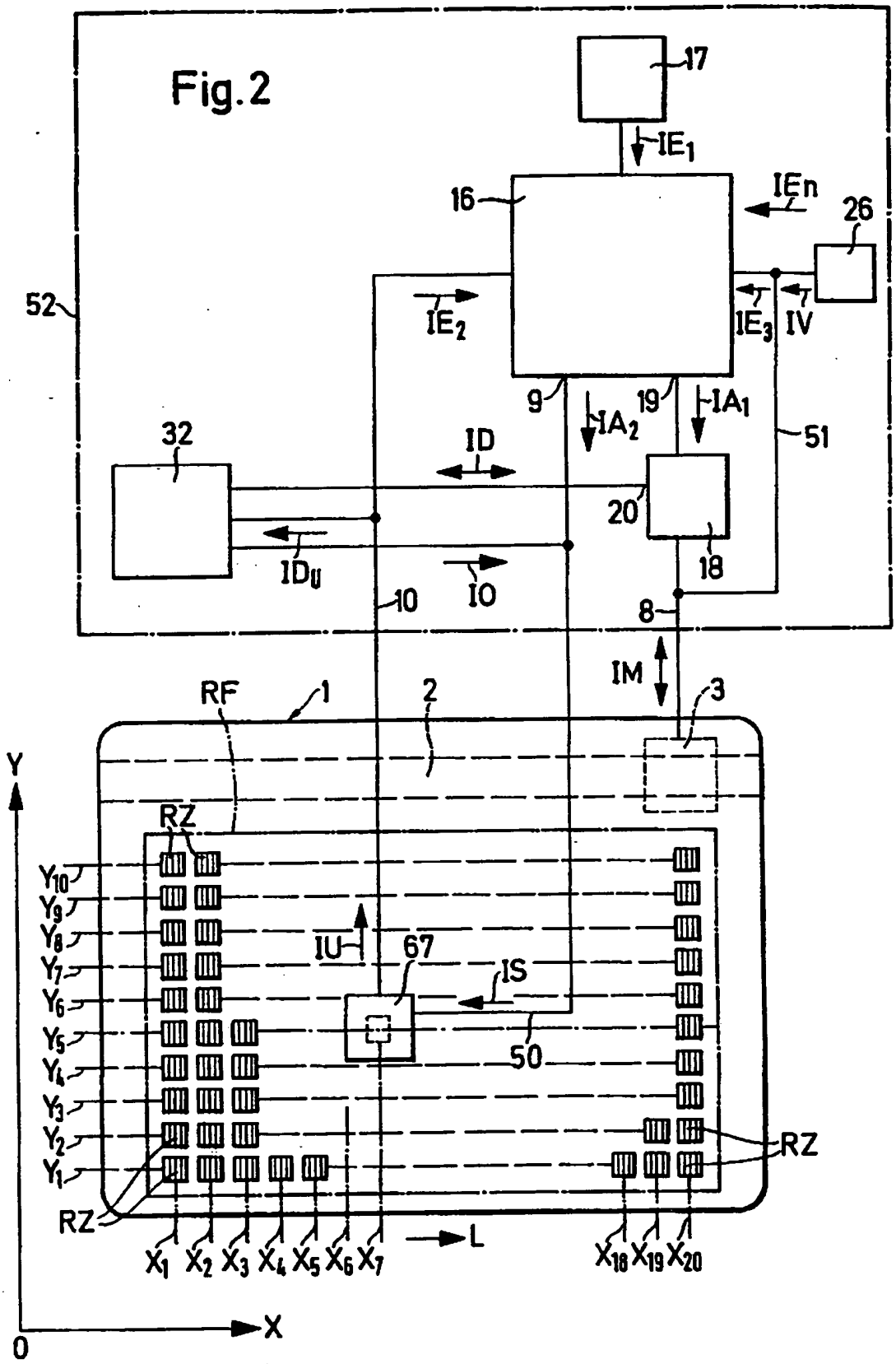


Fig.2


17
IE1
16
IEn
26
52
IE2
IE3
IV
9
IA2
19
IA1
51
32
ID
20
IDU
18
10
IO
8
IM
3
RF
1
2
Y
RZ
Y10
Y9
Y8
Y7
Y6
Y5
Y4
Y3
Y2
Y1
IU
67
IS
50
RZ
RZ
X1 X2 X3 X4 X5 X6 X7
L
X18 X19 X20
0
X

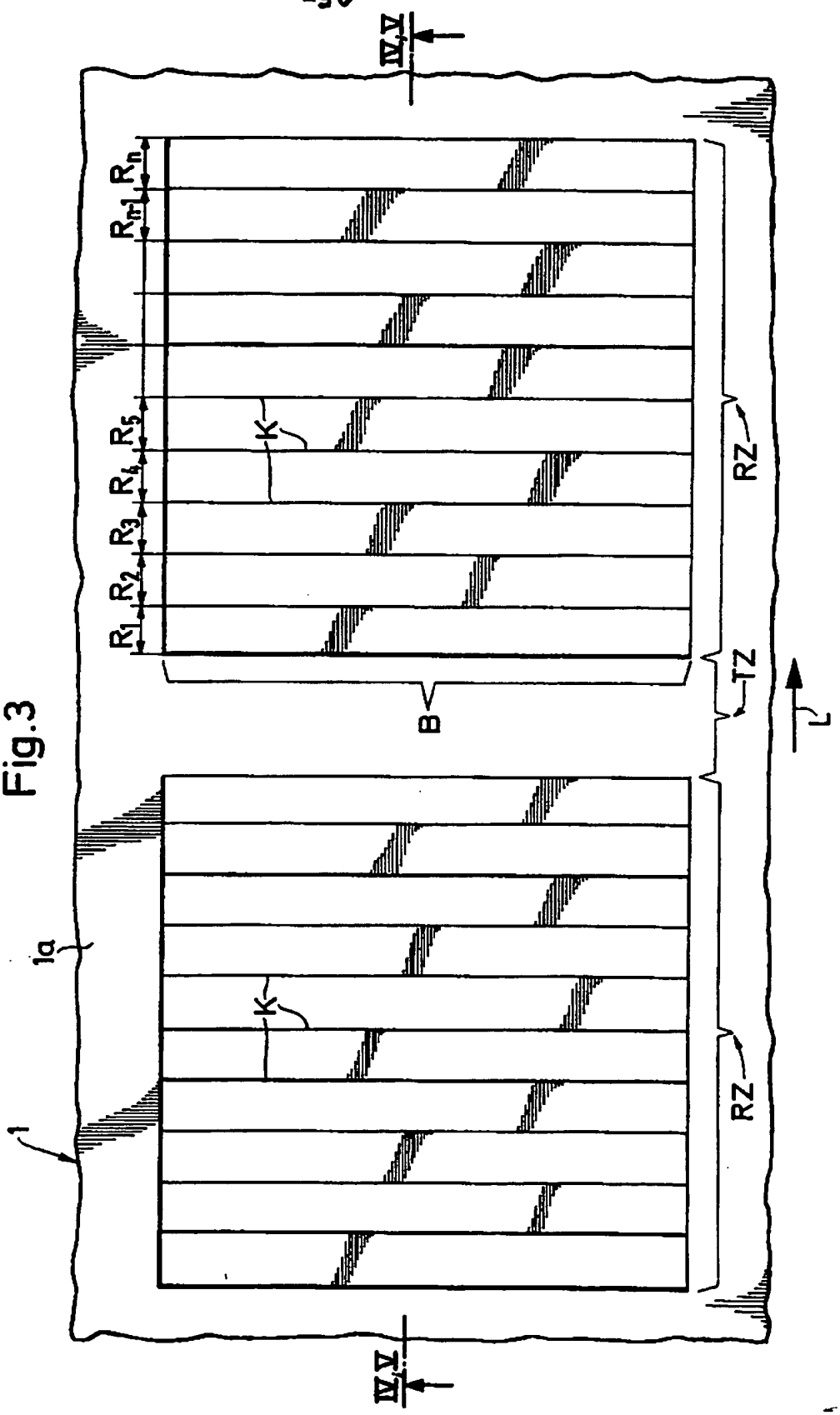


Fig.3

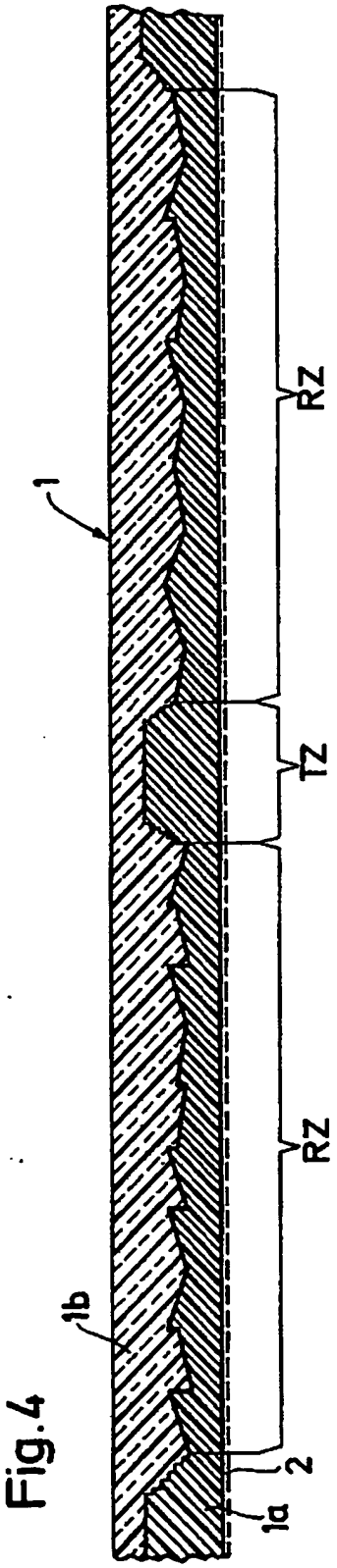


Fig.4

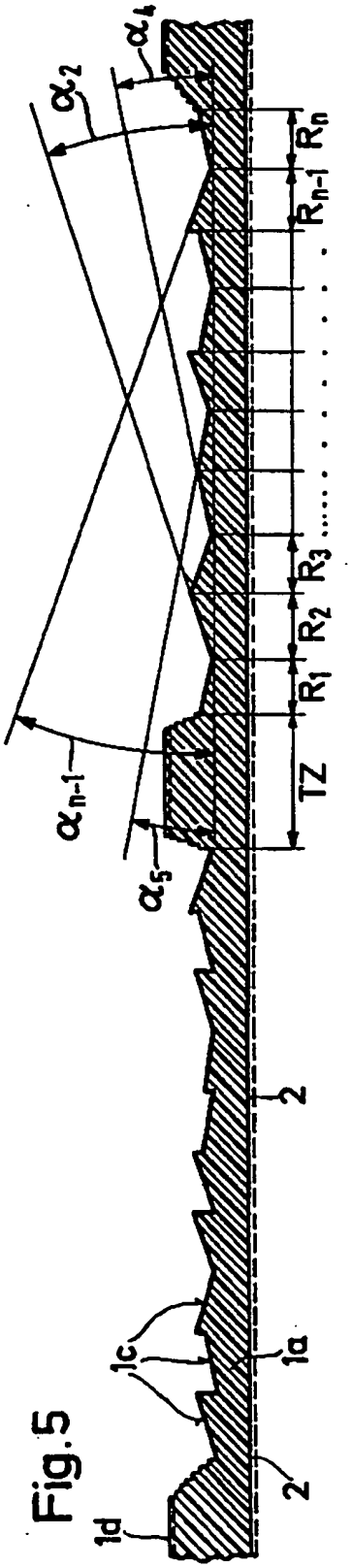
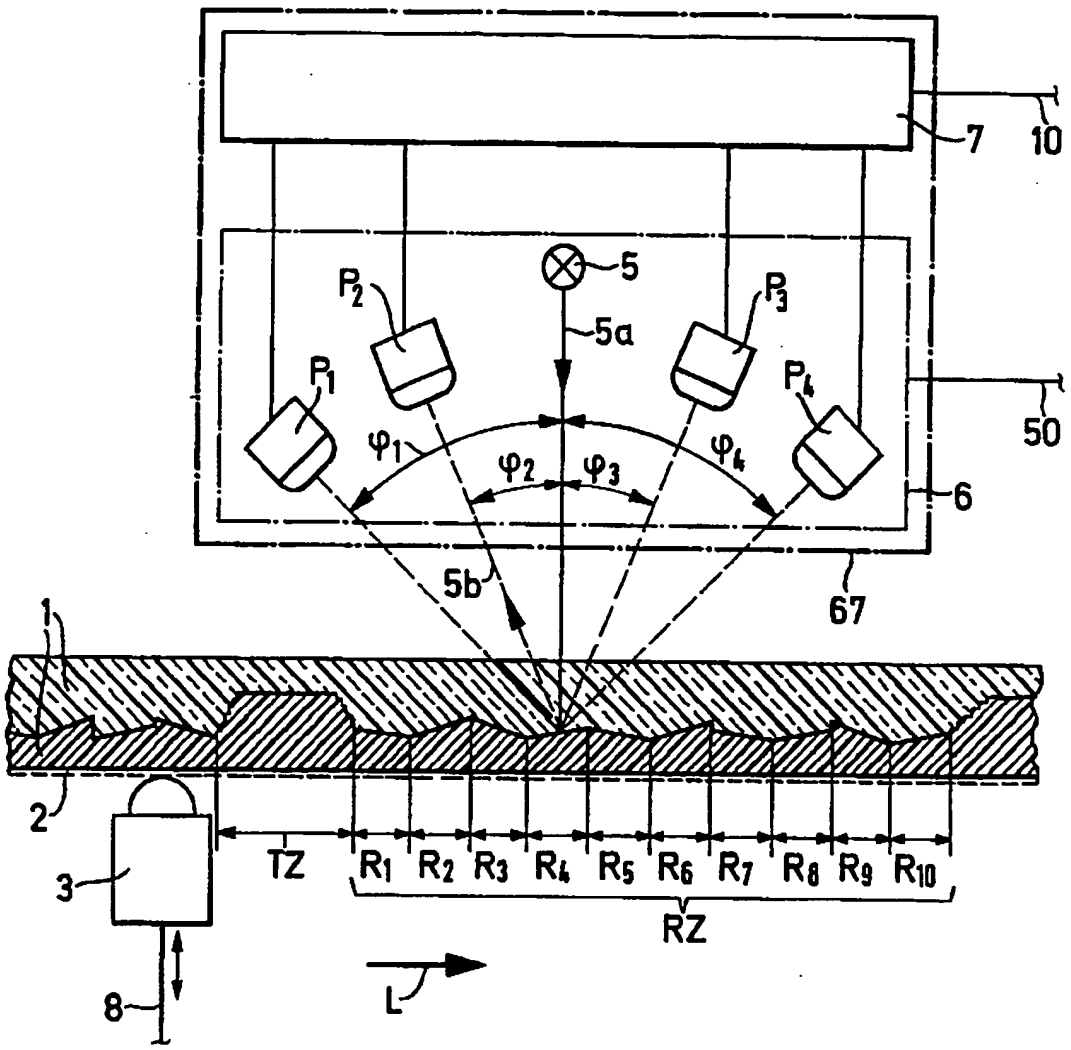


Fig.5

Fig.6


7
10
5
5a
P2
P3
P1
P4
φ1
φ2
φ3
φ4
50
6
5b
67
1
2
3
TZ
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10
RZ
L
8

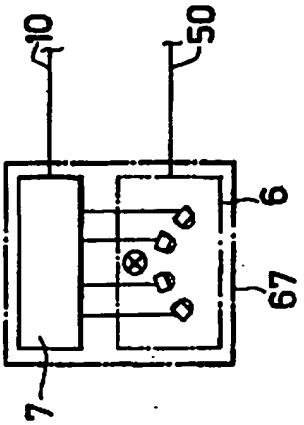

10
50
6
67
7
3
8
1
11
12
11a
13
2

Fig.7

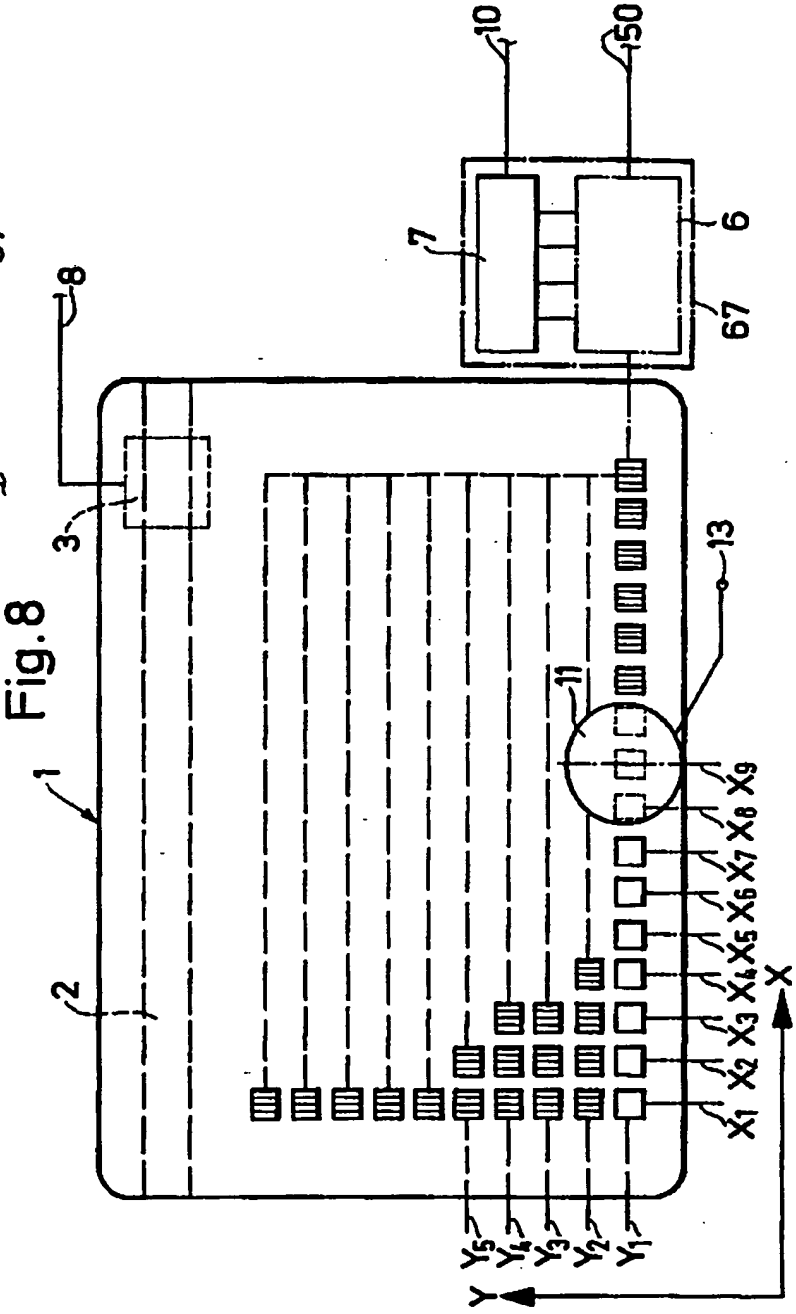
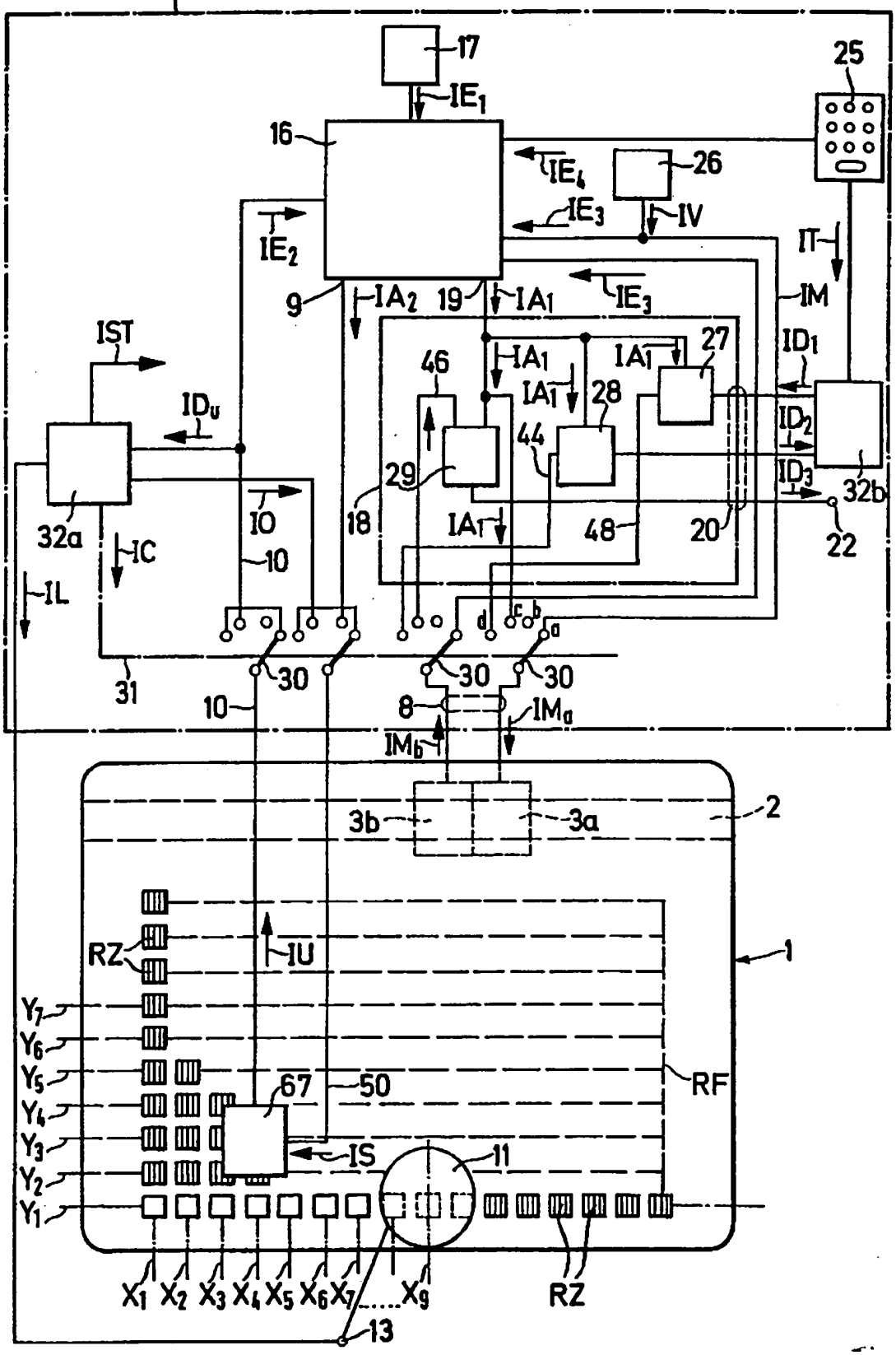

10
50
7
6
67
8
3
13
11
1
2
X9
X8
X7
X6
X5
X4
X3
X2
X1
X
Y5
Y4
Y3
Y2
Y1
Y

Fig.8

Fig.9


52
17
IE1
16
25
IE4
26
IE3
IV
IE2
IT
9
IA2
19
IA1
IE3
IM
IST
46
IA1
IA1
27
ID1
IDu
28
ID2
44
29
ID3
32b
32a
IC
10
18
IA1
48
20
22
IL
10
30
30
30
31
10
8
IMa
IMb
3b
3a
2
RZ
IU
1
Y7
Y6
Y5
Y4
Y3
Y2
Y1
67
50
RF
IS
11
X1 X2 X3 X4 X5 X6 X7 ..... X9
RZ
13